

**Canadian Association
of Chiefs of Police**

leading progressive change in policing



**Association canadienne
des Chefs de police**

à l'avant-garde du progrès policier

Office of the Secretary
Federal Communications Commission
445 12th St, S.W
Washington, D.C.20554

RECEIVED & INSPECTED

APR 19 2004

FCC - MAILROOM

Re: Comments Sought on CALEA Petition for Rulemaking RM-10865

I am writing on behalf of the Canadian law enforcement community to express support for the policy positions outlined in the United States Department of Justice, Federal Bureau of Investigation and Drug Enforcement Administration joint petition, on behalf of the United States law enforcement community, to resolve outstanding issues associated with the implementation of the *Communications Assistance for Law Enforcement Act* (CALEA). While we are not in a position to comment on the application of United States legislation, we are writing to underline the need expressed in the petition for governments to take prompt action to maintain law enforcement agencies' lawful intercept capabilities in the face of the rapid changes in telecommunication technologies.

Lawful interception is an essential and highly effective tool used to investigate serious crimes, such as drug trafficking, money laundering, smuggling, child pornography, and murder. It is also an essential tool for the investigation of threats to national security, such as terrorism. In Canada the conviction rate is over 90% in cases where lawful interception evidence is used in court.

However, rapidly evolving technologies such as broadband and wireless Internet access services and Voice Over Internet Protocol (VoIP) are increasingly challenging the ability of police agencies on both sides of the Canada-United States border to lawfully access the information needed to ensure public safety and national security. The worldwide adoption of these new telecommunications technologies and the increasingly global nature of crime and terrorism underpin the need for international cooperation in developing effective solutions.

Telecommunications service providers are now rolling out their 'next-generation' packet-mode networks. The use of Voice on the Internet is rapidly increasing. Businesses are replacing their PABX or Centrex networks with IP-based systems. VoIP is slowly being deployed in customer access networks and

No. of Copies rec'd _____
List ABCDE _____

several Internet Service Providers are known to be planning broadband telephony offerings as a replacement for their public switched telephone networks.

At the same time, the ability for the police to investigate crimes committed on, against or facilitated by the Internet is becoming essential to protecting public safety and critical infrastructures. The Internet is now a vital conduit for criminals. From 1997 to present, police services in Canada have seen an approximate increase of 300% in computer crime cases and a similar increase in the amount of interception authorizations for Internet communications. Criminals and terrorists are aware of our limitations to intercept new technologies and are exploiting this weakness to thwart investigative activities. As capabilities decline, law enforcement agencies are being forced to use undercover officers or agents, which puts more lives at risk.

For this reason, our respective laws must be flexible in order to adapt to new and emerging threats to public safety. It is important for the Governments of Canada and the United States to move forward promptly and in lock step to require that all technologies be made intercept capable. Joint action in setting clear deadlines for compliance with interception needs would minimize the costs to industry and governments by setting clear requirements, which can be implemented during the design stage of new technologies. Compelling all North American service providers to build and maintain this intercept capability would create a level playing field for industry and avoid the high cost of having to retrofit solutions after technologies such as broadband telephony have already been deployed.

When a new technology is introduced, police services often have to research and develop unique and costly tools to gain lawful access to those networks, only to find that criminals and terrorists have migrated to another technology. As raised earlier, broadband telephony networks and the associated technical standards are only now beginning to emerge. Consequently, when police services attempt to undertake a lawful interception on a packet-mode network, the equipment required to enable the interception varies from network to network and often requires a more complex solution. The lack of a solution, or the delay in the ability to use it, is hampering the ability of law enforcement agencies worldwide to fulfil their mandates.

Standards for packet and soft switching are progressing rapidly to enable broadband telephony services from different providers to be assembled into a consistent service for users. As new telecommunications technologies and new services are designed, equipment manufacturers will develop lawful access solutions to meet both Canadian and American requirements as well as worldwide markets, and as a result, the development costs for the will be less than if the

intercept capability were unique. Respective governments must act and cannot continue to permit telecommunications service providers to put public safety at risk by allowing them to stall in standards setting bodies.

For this reason, in 2002, the Government of Canada announced a legislative review and released a consultation paper on lawful access, which invited Canadians to submit views on these issues. The paper outlined proposals to ensure Canada's lawful access laws keep pace with new technologies ; ([http:// www.justice.gc.ca/en/cons/la_al/index.html](http://www.justice.gc.ca/en/cons/la_al/index.html)). Pursuant to this review, a new Act is being proposed in Canada that would compel all telephone and Internet service providers, including broadband access providers, to ensure that their systems have the technical capability to provide lawful access. Telecommunications service providers would be responsible for the costs associated with providing a lawful access capability for new technologies and when a significant upgrade is made to their existing systems.

Police services in Canada and the United States are not seeking expanded interception powers. The proposals being considered by the Government of Canada and before the FCC aim to maintain the ability of law enforcement and national security agencies to investigate serious crimes and threats to national security, including terrorism, committed with the aid of the Internet and other rapidly evolving telecommunications technologies. Simply put, information that has been available to law enforcement and national security agencies when criminals and terrorists used the mail, rotary phones and analog technologies should be available to them now.

The Canadian Association of Chiefs of Police and its members recognize that telecommunications service providers incur costs in providing assistance to police services. However, police services simply cannot afford the growing costs being charged by service providers for lawful access operational assistance. Cost recovery by telecommunications service providers for the deployment of interception solutions should be broadly and equitably distributed, as well as being reasonable and proportional to the actual assistance provided.

There is a public expectation that all sectors of the community, including the business community, have to work together to ensure public safety. In this regard, we support the principles voiced in the U.S. law enforcement agencies' submission that outlines that police services are different from other service providers' customers, that service providers should not profit from the assistance provided and that no entity should be permitted to limit the effectiveness of a court order. We support the U.S. agencies' position that any fees paid must reflect only cost recovery for the services provided and should not include cost recovery of the costs of deploying the infrastructure required to permit lawful interception, which

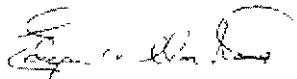
should be passed to the service providers' subscribers. Canadian law enforcement agencies are seeking this as part of the lawful access legislative review to ensure that these principles are similarly implemented in Canada.

The ability to implement court ordered interception must never be compromised. There should be no "intercept safe havens" in Canada or the United States. New technologies are not of themselves problematic. However, without the necessary checks and balances, they can have unintended detrimental consequences. Updated legal mechanisms are required to ensure that we, as a society, balance the needs of global competitiveness with those of effective public safety.

The matters at hand are not confined to jurisdictional boundaries. They are global issues that must be addressed in a comprehensive manner that transcends international borders. We believe that the ability to conduct electronic surveillance is in jeopardy due to the deregulated telecommunications environment and the plethora of new technologies available to the consumer.

We share a common border and common objectives such as facilitating the movement of legitimate goods and people, while preventing terrorists and criminals from entering Canada and the United States. However, police services will continue to face increasing challenges in meeting our shared goal to ensuring public safety and national security as long as the governments in Canada and the United States continue to allow new technologies such as broadband telephony to be deployed without any interception capabilities. To this end, the Canadian law enforcement community asks that you give serious consideration to supporting the policy proposals put forward in the United States law enforcement petition.

Respectfully submitted,



Chief Edgar MacLeod
President, Canadian Association of Chiefs of Police

c.c. John G. Malcolm
Deputy Assistant Attorney General,
Criminal Division
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

--

Patrick W. Kelly
Deputy General Counsel
Office of the General Counsel
Federal Bureau of Investigation
J Edgar Hoover Building
935 Pennsylvania Avenue, N.W
Room 7427
Washington, D.C. 20535

Robert T. Richardson
Deputy Chief Counsel
Office of Chief Counsel
Drug Enforcement Administration
Washington, D C. 20537